

EXHIBIT A

**IN THE CIRCUIT COURT OF THE 17TH JUDICIAL CIRCUIT
IN AND FOR BROWARD COUNTY, FLORIDA**

Case No.

MARIBEL CANCINO,

Plaintiff,

v.

AT&T CORPORATION,

Defendant.

COMPLAINT FOR DECLARATORY RELIEF

Plaintiff Maribel Cancino ("Plaintiff") sues AT&T Corporation ("Defendant") for declaratory relief with respect to a data breach suffered by Plaintiff.

JURISDICTION AND VENUE

1. This is an action for declaratory relief, pursuant to Chapter 86, Florida Statutes, seeking to declare that, among other things, personal and private information belonging to Plaintiff was held by Defendant and that said information breached and/or leaked to unauthorized parties from Defendant.

2. This Court has jurisdiction to grant declaratory under Fla. Stat. §§ 86.011, 86.021.

3. Venue in this District is proper because Plaintiff resides here, Defendant transacts business here, and the complained conduct of Defendant occurred here.

PARTIES

4. Plaintiff is a natural person, and a citizen of the State of Florida, residing in Broward County, Florida.

5. Defendant is a New York corporation, with its principal place of business located in Bedminster, New Jersey.

ALLEGATIONS

6. Defendant is an organization that provides, among other things, telecommunication services to consumers throughout the State of Florida on a for-profit basis (the “Services”).

7. Plaintiff paid Defendant an agreed upon amount for the Services.

8. In connection with the Services, Plaintiff was required to provide Defendant with certain private and sensitive information, such as Plaintiff’s name, address, phone number, date of birth, social security number, e-mail address, banking information, credit card information, as well as required Plaintiff to create a username and password (the “Sensitive Information”).

9. As custodian of the Sensitive Information, Defendant owed Plaintiff a duty to safeguard and prevent unauthorized third-parties access to the Sensitive Information.

10. On April 16, 2024, Defendant notified Plaintiff in writing that some or all of the Sensitive Information was leaked to, or otherwise accessed by, one or more unauthorized third parties. Attached as Exhibit “A” is a copy of said letter (the “Data Beach Letter”).

11. Defendant does not specify the specific information associated with Plaintiff that was leaked to, or otherwise accessed by, one or more unauthorized third parties.

12. Plaintiff must learn what specific information associated with Plaintiff was leaked to, or otherwise accessed by, one or more unauthorized third parties to take remedial action, of which includes notifying the credit reporting agencies that certain specific information belonging to Plaintiff is in the possession of unauthorized third parties.

13. Defendant does not affirmatively state whether the one or more unauthorized third party was an agent or employee of Defendant or a completely unknown entity.

14. Plaintiff must learn whether the one or more unauthorized third party was an agent or employee of Defendant or a completely unknown entity to properly understand the scope of the

damage sustained by Plaintiff and otherwise assess whether the severity of risk Plaintiff faces.

15. Defendant does not affirmatively state it has taken additional measures to ensure that any information belonging to Plaintiff that *was not* captured by one or more unauthorized third parties is safe from future unauthorized access.

16. Plaintiff must learn whether Defendant has taken any action to prevent future unauthorized access to the Sensitive Information so Plaintiff can properly take independent action to protect Plaintiff's best interest.

17. Defendant does not affirmative state how unauthorized third parties were able to gain access to the Sensitive Information.

18. Plaintiff must learn how unauthorized third parties were able to gain access to the Sensitive Information so Plaintiff can properly take independent action to protect Plaintiff's best interest.

19. Plaintiff requires a declaration from this Court as to Plaintiff's status as a victim of a data breach, the specific information which was leaked and/or accessed by unauthorized third parties, and the date and method of the data breach, so that Plaintiff can properly exercise rights enjoyed under the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*, as well as take independent measures to safeguard against identity theft, rebut fraudulent use of the Sensitive Information, and file a detailed police report with local authorities.

COUNT 1
DECLARATORY RELIEF

20. Plaintiff incorporates by reference paragraphs 6 through 19 of this Complaint.

21. "In order to invoke jurisdiction under the Declaratory Judgment Act, the complaint must show that there is a bona fide, actual, present and practical need for the declaration; that the declaration will deal with present, ascertained or ascertainable state of facts, or present controversy

as to a state of facts; that some immunity, power, privilege or right is dependent upon facts or law applicable to facts; that there is some person or persons who have, or reasonably may have, an actual, present, adverse and antagonistic interest in the subject matter, either in fact or law; that the antagonistic and adverse interests are all before the court; and that the relief sought is not merely the giving of legal advice by the courts or the answers to questions propounded from curiosity.” Connelly v. Old Bridge Vill. Co-Op, Inc., 915 So. 2d 652, 655 (Fla. 2nd DCA. 2005)

22. Broad interpretation is to be given to the Declaratory Judgment Act Olive v. Maas, 811 So. 2d 644 (Fla. 2002). *Citing Merle Wood & Assocs. v. Intervest-Quay Ltd. P'ship*, 877 So. 2d 942, 943 (Fla. Dist. Ct. App. 2004).

23. As stated above, Defendant notified Plaintiff in writing that Plaintiff's private and sensitive information was leaked to, or accessed by, unauthorized third parties. Plaintiff requires the specifics as to said unauthorized access and/or leaking of Plaintiff's private and sensitive information so that Plaintiff.

24. Plaintiff requires a declaration from this Court as to Plaintiff's status as a victim of a data breach, the specific information which was leaked and/or accessed by unauthorized third parties, and the date and method of the data breach, so that Plaintiff can properly exercise rights enjoyed under the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*, as well as take independent measures to safeguard against identity theft, rebut fraudulent use of the Sensitive Information, and file a detailed police report with local authorities.

25. WHEREFORE, Plaintiff asks that this Court declare: [1] Plaintiff was the victim of a data breach; [2] Defendant leaked and/or breached information belonging to Plaintiff to an unauthorized party or parties; [3] The specific information leaked and/or breached belonging to

Plaintiff; [4] The information held by Defendant belonging to Plaintiff that was not leaked or beached; [5] The date of the data breach; and [6] How and/or why the data breach occurred.

DATED: June 5, 2024

Respectfully Submitted,

/s/ Thomas Patti

THOMAS PATTI, ESQ.

Florida Bar No. 118377

E-mail: Tom@pzlg.legal

PATTI ZABALETA LAW GROUP

110 SE 6th Street Suite 1732

Fort Lauderdale, Florida 33301

Phone: 561-542-8550

COUNSEL FOR PLAINTIFF

EXHIBIT A

From: AT&T <ATT@message.att-mail.com>
Date: Tue, Apr 16, 2024, 12:00 PM
Subject: Important Information
To: <marguandino@gmail.com>



AT&T Security Update

Hello,

We're contacting you regarding the security of your data. After a thorough assessment, AT&T has determined that some of your personal information was compromised. This data does not include personal financial information or call history.

What is AT&T doing to help?

AT&T takes these issues very seriously. We are offering you one year of complimentary credit monitoring, identity theft detection and resolution services, provided with IdentityWorksSM. Please follow the instructions below and **enroll by August 30, 2024**.

Where can you get more information?

Visit att.com/accountsafety for more details.

We apologize this has happened.

AT&T

Experian's[®] IdentityWorksSM

AT&T is providing you with an IdentityWorksSM membership at no charge. After you complete registration, you'll have increased visibility into potential fraud up to \$1,000,000 in coverage should you experience identity theft and an Identity Restoration team to guide you through the recovery process.

To activate your membership and start monitoring your personal information, please follow the steps below:

- **Enroll** by August 30, 2024 (Your code will not work after this date.)
- **Go** to the [Experian's[®] IdentityWorksSM](#) website and select 'Get Started'
- **Enter** your activation code: **79TPQ5VN6**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian's[®] IdentityWorksSM online, call 833.931.4853 by **August 30, 2024**. Be prepared to provide this engagement number (**B119859**) as proof of eligibility for the identity restoration services.

[My Account](#) | [Help Center](#) | [Terms of Use](#) | [Contact Us](#)

To ensure the delivery of AT&T emails to your inbox, please add att@message.att-mail.com to your email address book or safe senders list.

View AT&T's [Privacy Policy](#).

© 2024 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo, all other AT&T marks contained herein are trademarks of AT&T Intellectual Property. All other marks are the property of their respective owners.

A2837837 | A000000030